UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

LINDABETH RIVERA, on behalf of herself and all others similarly situated, Plaintiff, v. GOOGLE INC., Defendant.	Civil Action No. 1:16-cv-2714 Hon. Edmond E. Chang Magistrate Michael T. Mason
JOSEPH WEISS, individually and on behalf of all others similarly situated, Plaintiff, v. GOOGLE INC., Defendant.	Civil Action No. 1:16-cv-02870 Hon. Edmond E. Chang Magistrate Michael T. Mason

PLAINTIFFS' RESPONSE IN OPPOSITION TO
GOOGLE'S CONSOLIDATED MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

Plaintiffs Lindabeth Rivera and Joseph Weiss, on behalf of themselves and the putative class, submit this response in opposition to the consolidated motion to dismiss (D.E. 49 (the "Motion to Dismiss")) the first amended complaints (D.E. 41-42 (the "Complaints")) filed by Google, Inc. ("Google").

INTRODUCTION

In enacting the Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1 to 14/99 (West, Westlaw through P.A. 99-324 of 2015 Reg. Sess.), Illinois banned unauthorized gathering of two distinct and separately defined things: (1) "biometric identifiers," which are defined as retinal scans, iris scans, voiceprints, fingerprints, and scans of hand or face geometry; and (2) "biometric information," i.e., any information based on a biometric identifier. Google gathers biometric identifiers – specifically, scans of face geometry – from millions of individuals without consent. Google therefore violates the statute.

Google does not deny that it gathers scans of face geometry without consent. Instead, it argues that scans of face geometry are not biometric identifiers if they are derived from photographs rather than in person, because the definition of biometric information excludes information derived from photographs. As two district courts recently concluded, this argument fails for several reasons. *See Norberg v. Shutterfly, Inc.*, --- F. Supp. 3d ---, 2015 WL 9914203 (N.D. Ill. Dec. 29, 2015) (Norgle, J.); *In re Facebook Biometric Info. Privacy Litig.*, No. 15-CV-03747-JD, --- F. Supp. 3d ---, 2016 WL 2593853 (N.D. Cal. May 5, 2016). First, the exception for derivatives of exclusions pertains only to the definition of biometric information, not biometric identifiers. Scans of face geometry are biometric identifiers, not biometric information. Second, the statute says nothing about gathering biometric identifiers in person, and in fact expressly regulates biometric identifiers regardless of derivation. Third, it would be senseless to permit unauthorized scanning from photographs but not in person. All of the biometric identifiers covered by the statute are

obtained from visual or audio media. If the intermediation of a photograph or audio recording excused all subsequent processing into a biometric identifier, Google's interpretation of the exception would swallow the rule.

Google additionally argues that Plaintiffs' claims exceed the geographical scope of the statute and, alternatively, that the statute violates the dormant commerce clause. These arguments are also without merit. While it is true that BIPA does not apply extraterritorially (i.e., beyond the boundaries of Illinois), in this case Google violated BIPA in Illinois because the overwhelming majority of circumstances relating to the violations occurred there. Plaintiffs are Illinois residents whose biometric identifiers were automatically collected by Google without consent from photos taken in Illinois and immediately thereafter uploaded in Illinois. BIPA does not impose any substantial burden on interstate commerce in violation of the dormant commerce clause because companies such as Google, in order to comply with the statute, need only refrain from collecting scans of face geometry without consent from individuals appearing in photographs uploaded within the state of Illinois.

Google is free to gather photographs, and is free to gather information from photographs, but Google is not free to gather biometric identifiers from photographs uploaded in Illinois. The Motion to Dismiss should be denied.

APPLICABLE LEGAL STANDARDS

On a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a court "must construe [the complaint] in the light most favorable to plaintiff, accept well-pleaded facts as true, and draw all inferences in the plaintiff's favor." *Carlson v. CSX Transp., Inc.*, 758 F.3d 819, 826 (7th Cir. 2014).

When interpreting state law, a federal court applies the rules of statutory construction

applicable under state law. *See U.S. Fire Ins. Co. v. Barker Car Rental,* 132 F.3d 1153, 1156 (7th Cir. 1997) ("[W]e must apply the same rules of statutory construction that the Supreme Court of Illinois would apply if it were faced with the same task."). "In Illinois, the applicable principles of statutory construction are well established. The primary rule is that courts should ascertain and give effect to the intention of the legislature. To achieve that goal, we must regard the language of the statute as the best indication of legislative intent." *U.S. Fire Ins.*, 132 F.3d at 1156 (citing *Abrahamson v. Ill. Dep't of Prof'l Regulation,* 153 Ill. 2d 76, 90 (1992)); *see also DeLuna v. Burciaga*, 223 Ill. 2d 49, 59 (2006) ("When the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation."). Courts "will not depart from the plain statutory language by reading into the statute exceptions, limitations, or conditions that the legislature did not express." *People v. Lewis*, 223 Ill. 2d 393, 402 (2006) (citation omitted).

Where a statute requires interpretation and the exact legislative intent cannot be ascertained from the plain and ordinary meaning of its language alone, the court is guided by the canons of statutory construction and by legislative history, *People v. Holm,* 387 Ill. Dec. 616, 619 (Ill. App. Ct. 2014), and also by the practical consequences of the competing statutory interpretations, *Jordan v. Dominick's Finer Foods*, No. 10 C 407, 2015 WL 4498909, at *2 (N.D. Ill. July 23, 2015).

THE BIOMETRIC INFORMATION PRIVACY ACT

Section 10 of BIPA states:

> 'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. . . .
>
> 'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from

> items or procedures excluded under the definition of biometric identifiers.

740 Ill. Comp. Stat. 14/10 (emphasis added). BIPA prohibits possessing, capturing, collecting, purchasing, receiving through trade, or otherwise obtaining an individual's biometric identifiers or biometric information, absent express consent from the individual following a written disclosure of the collection and a public policy for handling and disposing of such data. 740 Ill. Comp. Stat. 14/15(a)-(d).[1]

ARGUMENT

The Complaints allege claims for violation of BIPA that are consistent with the plain statutory language. BIPA does not violate the dormant commerce clause because the statute does not regulate conduct, let alone impact commerce, outside of Illinois. The Motion to Dismiss should be denied.

I. Google's Argument That BIPA Does Not Cover Scans Of Face Geometry Derived From Photographs Disregards the Plain Statutory Language and Is Contrary To The Legislative Intent.

The plain language of BIPA defines Google's scans of face geometry to be biometric identifiers. This conclusion is confirmed by the canons of statutory construction and the legislative history.

1. Scans of Face Geometry Derived From Photographs Are Biometric Identifiers Under The Plain and Ordinary Meaning of BIPA

Under the plain language of BIPA, the definition of "biometric identifiers" includes "scans of . . . face geometry." 740 Ill. Comp. Stat. 14/10. The definition does not contain any

[1] Each BIPA restriction (*i.e.,* collection, possession and use) applies disjunctively to both biometric information and biometric identifiers. *See* 740 Ill. Comp. Stat. 14/15(a) ("A private entity in possession of biometric identifiers ***or*** biometric information must develop a written policy . . .); 740 Ill. Comp. Stat. 14/15(b) ("No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier ***or*** biometric information, unless it first . . .").

qualification relating to how the identifier was derived. Therefore, on its face, the statute encompasses biometric identifiers – i.e., scans of face geometry – derived from human faces depicted in photographs.

The Complaints are entirely consistent with the clear and unambiguous statutory language. The Complaints allege that Google's sophisticated, patented facial recognition technology searches each and every user-uploaded photo for faces, and then scans those faces for geometric points and contours for purposes of creating and storing a digitized face template of each face. (*Rivera* Compl. ¶¶ 21-22, 27-28; *Weiss* Compl. ¶¶ 21-22, 28-29.) The resulting face templates – not the innocuous photographs from which they were derived, but the resulting highly detailed digital maps of geometric points and measurements – are "scans of face geometry" and thus fall within BIPA's definition of "biometric identifiers." (*Id.*)[2]

Google attempts to overcome the plain meaning of the statute in two ways. First, it points out that the definition of biometric identifiers excludes photographs, and then conflates this with the definition of "biometric information," which excludes information derived from items (such as photographs) that are excluded from the definition of biometric identifiers. This misses the mark. Information derived from photographs is excluded from the definition of biometric information, not from the definition of biometric identifiers. The Complaints allege that Google gathers biometric identifiers (scans of face geometry) from photographs. Google's argument therefore fails under the plain language of the statute. *See DeLuna*, 223 Ill. 2d at 52.

---

[2] The Complaints also allege that Google collects "biometric information" (pertaining to gender, age and location) that is derived from the resulting "scans of face geometry." (*Rivera* Compl. ¶ 44; *Weiss* Compl. ¶ 45.) Because such information is derived from "biometric identifiers" as opposed to the photographs themselves, Google's unauthorized collection of this information also constitutes a violation of BIPA. *See* 740 Ill. Comp. Stat. 14/10; 740 Ill. Comp. Stat. 14/15(a)-(d).

Second, Google argues that BIPA regulates only "in-person" collection of biometric identifiers, not collection from photographs. The definition of biometric identifiers, however, contains no reference whatsoever to the source of the identifier. There is neither a requirement of in-person collection nor an exclusion of photographic collection. Moreover, on its face, the statute regulates biometric identifiers regardless of derivation: "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier[.]" 740 Ill. Comp. Stat. 14/15 (emphasis added). Google's argument to the contrary improperly "read[s] into the statute exceptions, limitations or conditions that the legislature did not express." *Lewis*, 223 Ill. 2d at 402. Again, Google's argument fails under the plain language of the statute.

Two recent district court decisions interpreting BIPA confirm this conclusion. In *Shutterfly* and *In re Facebook*, both district courts carefully considered, and rejected, all of the same arguments raised by Google in the Motion to Dismiss, and held that scans of face geometry derived from photographs constitute "biometric identifiers" under the plain language of BIPA. The court in *Facebook* explained:

> BIPA regulates the collection, retention, and disclosure of personal biometric identifiers and biometric information by '[m]ajor national corporations,' among others. *See* 740 Ill. Comp. Stat. 14/5(b), (g); Section I.C.2(B), above. It defines 'biometric identifier' as 'a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.' 740 Ill. Comp. Stat. 14/10. Plaintiffs allege that Facebook scans user-uploaded photographs to create a 'unique digital representation of the face...based on geometric relationship of their facial features.' That allegation falls within the scan of face geometry stated in the statute.

In re Facebook Biometric Info. Privacy Litig., 2016 WL 2593853, at *12. Judge Norgle in *Norberg* likewise based his decision on BIPA's plain language. *See Norberg*, 2015 WL 9914203, at *2 ("Turning to the

plain language of the statute," and holding that allegations that defendant collected scans of face geometry from user-uploaded photographs "plausibly state[s] a claim for relief under BIPA.").

Though the Motion to Dismiss says to "[s]tart with the statute's text" (Mot. at 7), Google ignores its own directive by immediately turning to the statutory construction and legislative history, without even attempting to dispute that scans of face geometry derived from photographs – items which are not excluded from the definition of biometric identifiers – "fall[] within the scan of face geometry stated in the statute." *In re Facebook Biometric Info. Privacy Litig.*, 2016 WL 2593853, at *12. Because the statutory language is clear in this regard, the Court need go no further in its analysis. *See DeLuna*, 223 Ill. 2d at 59 ("When the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation.").

The Complaints state a claim, and the Motion to Dismiss should be denied.

2. Statutory Construction and Legislative History Confirm BIPA's Applicability to Scans of Face Geometry Obtained from Photographs

Proper statutory construction and the legislative history confirm that BIPA prohibits unauthorized gathering of biometric identifiers from photographs or other media, no less than unauthorized gathering of identifiers in person. All biometric identifiers are subject to the statute, regardless of derivation.

a. Statutory Construction

Canons of statutory construction – including statutory language and structure, extrinsic meanings of relevant terms, and the practical consequences of Google's alternative interpretation – all confirm that the statute prohibits gathering scans of face geometry from photographs (or from any other source) without consent.

i. Statutory Language and Structure

"A fundamental principle of statutory construction is to view all provisions of a statutory enactment as a whole. Accordingly, words and phrases should not be construed in isolation, but must be interpreted in light of other relevant provisions of the statute." *S. Illinoisan v. Illinois Dep't of Pub. Health*, 218 Ill. 2d 390, 415 (2006); *see also Jordan,* 2015 WL 4498909, at *2 ("[T]he statutory 'text' must be placed within its 'context' to be properly understood.").

Accordingly, differences in statutory language must be given force and effect, especially in adjacent provisions where parallel terms would be expected if truly intended. Thus, the Illinois Supreme Court reasoned in *Bruso by Bruso v. Alexian Brothers Hospital*, 178 Ill. 2d 445 (1997):

> Subsection (c) is clearly intended to act as an exception to both subsections (a) and (b). If the legislature had intended legal disability to be an exception for adults only, the logical place for that exception would have been in, or immediately following, subsection (a). The legislature, however, chose to locate the tolling provision for legal disability in a separate subsection following subsections (a) and (b).

178 Ill. 2d at 453. Similarly, the Court reasoned in *DeLuna*:

> If the legislature had intended subsection (e) of section 13–214.3 to apply only to the statute of limitations contained in subsection (b), it could have placed that tolling provision 'in, or immediately following,' subsection (b). However, the legislature chose, instead, to locate the tolling provision for minors in a separate subsection following subsections (b) and (c). It is, therefore, reasonable to infer that it was meant to apply to both.

223 Ill. 2d at 63-64.

In this case, the definitions of "biometric identifier" and "biometric information" differ at exactly the point where Google has placed all its chips. The definition of biometric identifiers contains a long list of items (such as photographs) that are excluded. 740 Ill. Comp. Stat. 14/10. None of the many exclusions, however, says anything about identifiers derived from those exclusions. The definition of "biometric information," by contrast, contains just one simple

exclusion: "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.* Thus, the statute explicitly excludes such derivatives from the definition of biometric information, *but not* from the separate definition of biometric identifiers.

Notably, the words "identifiers" and "information" are separately defined and consistently used in a manner that confirms the exclusion of derivatives pertains only to biometric information, not biometric identifiers. The statute provides: "Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id.* (emphasis added). The statute does not, however, exclude derivatives of the biometric identifier exclusions from the definition of biometric identifiers.

The Court must give meaning to these significant differences in statutory language and structure. The legislature could easily have provided for derivatives to be excluded from the definition of biometric identifiers, just as they are from the definition of biometric information. A parallel exclusion could have simply read: "Biometric identifiers do not include identifiers derived from items or procedures excluded under this definition of biometric identifiers." Or, as explained by *Bruso* and *DeLuna*, a single exclusion could have covered both definitions: "Biometric identifiers and biometric information do not include identifiers or information derived from items or procedures excluded under the definition of biometric identifiers." But there is no such exclusion. The legislature's decision to place an exclusion for derivatives solely in the definition of biometric information is clear evidence that the legislature intended for biometric identifiers to be regulated regardless of derivation. Accordingly, as the decisions in *Facebook* and *Shutterfly* confirm, a scan of

face geometry derived from a photograph constitutes a biometric identifier no less than any other scan of face geometry.[3]

Google argues that the phrase "scan of . . . face geometry", read together with the other listed biometric identifiers, somehow describes "a scan of the geometry of a person's actual face" that "must be derived from the person itself." (Mot. at 7-8.) But considered alongside the statute's regulatory provision – "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information," 740 Ill. Comp. Stat. 14/15 – this argument is completely meritless. As previously discussed, the catch all phrase "or otherwise obtain" clearly expresses the intent of the legislature to regulate biometric identifiers from any source, however obtained, in person or otherwise (and to regulate biometric information from any source, except from an excluded identifier).

Google's manufactured in-person collection requirement is also plainly at odds with the statute's expressed application to biometric identifiers "purchase[d]" and "receive[d] through trade," which underscores that the legislature intended to regulate biometrics regardless of origin. How a biometric identifier is "otherwise obtain[ed]" by Google – whether in person or from a photograph – makes no difference; it is a biometric identifier nonetheless.

---

[3] Google nevertheless contends that, "by excluding [information derived from photographs] from 'biometric information,' [the General Assembly] sought to ensure that such information would not be covered by the statute at all." (Mot. at 14.). As discussed above, this argument is contrary to BIPA's plain language and finds no purchase in the canons of statutory construction. Scans of face geometry derived from photographs are biometric identifiers, not biometric information, and are therefore clearly covered by the statute. However, even assuming Google were correct that the statute somehow excludes scans of face geometry derived from "photographs" from the definition of biometric identifiers (and it plainly does not), the "photographs" themselves that are excluded from the definition of biometric identifiers are "better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet." *In re Facebook Biometric Info. Privacy Litig.*, 2016 WL 2593853, at *12. Because the photographs at issue in this case were digital images that were uploaded to the Internet, the scans of face geometry derived from those images constitute biometric identifiers even under Google's erroneous reading of the statute. *See id.* ("Consequently, the Court will not read the statute to categorically exclude from its scope all data collection processes that use images.").

The Complaints state a claim, and the Motion to Dismiss should be denied.

ii. Extrinsic Definitions

Extrinsic definitions of statutory terms, especially technical terms, are properly considered in statutory construction. *See Jordan*, 2015 WL 4498909, at *2 (stating that when a term "is not defined by the statute itself" or "by any applicable case law interpreting the statute," it is "appropriate to employ a dictionary to ascertain the meaning of an otherwise undefined word or phrase") (citing *Landis v. Marc Realty, L.L.C.*, 235 Ill. 2d 1, 8 (2009)); *Gridley v. Gridley*, 399 Ill. 215, 223 (1948) ("Technical words, or words of known legal import, must have their legal effect[.] When unexplained and uncontrolled by the context they are to be interpreted according to their technical meaning."). "Biometric identifier" is a term of art that would generally be understood to exclude ordinary photographs but include technologically-enhanced identifiers derived from photographs.

The term "biometrics" is defined as "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity." Biometrics, Merriam-Webster, www.merriam-webster.com/dictionary/biometrics (last visited Dec. 17, 2015). Biometrics are characterized by the use of enhanced tools of measurement and analysis made possible by modern computing technology. *See generally* Steven C. Bennett, *Privacy Implications of Biometrics*, Prac. Law., June 2007, at 13, 14-15 ("The rise of mechanical biometric technology, especially computers and computerized databases, and the consequent automation of the identification process have radically increased both the ability to identify individuals biometrically and the potential for abuse of biometrics."); *see also* Public Access Opinion No. 14-008, 2014 WL 4407615, at *4 (Ill. Att'y Gen. Aug. 19, 2014) (stating, in context of Illinois FOIA statute, that "any clear photo of a person contains some

biometric information," but a photo does not qualify as a biometric identifier "in the technical or legal sense" unless there is an "intention to convert it to a template or match it against a face gallery" (emphasis added)).

In keeping with this ordinary understanding, BIPA regulates the use of such technologically enhanced "measurement and analysis" to collect individuals' unique identifying characteristics. *Id.* BIPA regulates scans of the retina or iris, fingerprints, voiceprints, and scans of hand or face geometry, however they are obtained, all of which employ technological measurement and analysis to ascertain identity. *See* 740 Ill. Comp. Stat. 14/10. Conversely, BIPA explicitly does not regulate commonplace and readily observable items that do not employ technologically enhanced tools of measurement and analysis to ascertain identity – items such as signatures, photographs and physical descriptions such as height, weight, hair color and eye color, *see id.*

Both the statute and the general definition of biometrics thus distinguish between technologically enhanced identifiers and commonplace items. The statute expresses the legislature's judgment that technologically enhanced identifiers require regulation. This fully explains the legislature's decision to regulate identifiers regardless of derivation. It is the use of enhanced "measurement and analysis" that necessitated legislative action. The enhanced measurement and analysis embodied in a biometric identifier (such as a scan of face geometry) derived from a photograph obtained second-hand is no different from (nor is it less invasive than) the enhanced measurement and analysis embodied in a biometric identifier obtained in person. The statute therefore applies equally to both.

In this case, the Complaints allege that Google developed and implemented sophisticated technological tools of measurement and analysis to create millions of biometric identifiers – unique face prints – and then applied further tools of measurement and analysis to match those face prints

against faces appearing in newly uploaded photographs. (*Rivera* Compl. ¶¶ 5, 21-22, 27-29, 34, 43; *Weiss* Compl. ¶¶ 5, 21-22, 27-30, 35, 44.) Google thus "collect[s], capture[s], purchase[s], receive[s] through trade, or otherwise obtain[s]," 740 Ill. Comp. Stat. 14/15(b), as well as "possess[es]," 740 Ill. Comp. Stat. 14/15(a), biometric identifiers without proper consent in violation of BIPA. (*Rivera* Compl. ¶¶ 24-25, 34, 43-48; *Weiss* Compl. ¶¶ 24-25, 35, 44-49.)

The Complaints state a claim, and the Motion to Dismiss should be denied.

iii. Practical Consequences

The practical consequences of a statutory interpretation are a strong indication of whether it is correct. *Jordan*, 2015 WL 4498909, at *2. In this case, Google's argument that the statute applies only to scans of face geometry from in-person interaction is belied by the practical consequences of such an interpretation.

The statute defines biometric identifiers as including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 Ill. Comp. Stat. 14/10. Every single one of those identifiers depends in the first instance on the capture of a photograph or, in the case of a voiceprint, an audio recording.

Photographs are the raw material used by Google and others to create scans of face geometry in the use of facial recognition technology:

> Generally, the automatic face recognition process begins with an analysis of 'training images' of already known individuals and measurement of their facial features. These measurements – which make up the individuals' unique biometric data – are compiled into a biometric database along with other known information about them. Face recognition technology is then applied to a new photo to find faces and identify them. If it detects any faces in that photo, it 'normalizes' them, which involves transforming their scale, position, and lighting, and sometimes converting them into gray scale images so that they can more easily be compared to faces photographed under different conditions. The technology then identifies and measures facial features in the normalized faces. The resulting

> measurements are compared to biometric data in the previously compiled database to identify the faces detected in the new **photo**.

Yana Welinder, *A Face Tells More Than A Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 Harv. J.L. & Tech. 165, 171 (2012) (emphasis added); *see also, e.g.,* Elizabeth M. Walker, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 Fordham Intell. Prop. Media & Ent. L.J. 831, 849-50 (2015) ("Many individuals . . . lack an understanding of how privacy and security are affected by technology. . . . [B]iometrics can be captured without an individual's knowledge. A fingerprint can be lifted from another object, gait can be recorded from a distance, and face and voice samples are easily captured by cameras, phones, and other devices."); Douglas A. Fretty, *Face-Recognition: A Moment of Truth for Fourth Amendment Rights In Public Places*, 16 Va. J.L. & Tech. 430, 454 (2011) ("For FRT [face recognition technology] to function, the state needs pre-labeled photographs of its citizens, and the gathering of these photographs may implicate federal law as well as the Fourth Amendment. Governments already have proprietary control over four major sources of facial photos: arrestee mug shots, passport photos, driver's license photos, and border-entry photos of non-citizens. Agencies can be expected to exploit these resources to support FRT to the maximum extent allowed by law.") (emphasis added).

Retina and iris scans are likewise based in the first instance on photographs. *See, e.g.*, Stephen Hoffman, *Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century*, Syracuse Sci. & Tech. L. Rep., Spring 2010, at 38 (explaining that in retinal scanning technology, "the camera photographs the vasculature structure of your eyes and runs it against a database"); *Lebowitz v. City of New York*, No. 12 CIV. 8982 JSR, 2014 WL 772349, at *2 (S.D.N.Y. Feb. 25, 2014) ("Iris scans are high resolution photographs of the pigmented portion of the eye, and are more accurate than fingerprints in confirming identity."), *aff'd*, 606 F. App'x 17 (2d Cir. 2015).

Fingerprint recognition systems, too, are based in the first instance on photographs. *See, e.g.*, Michael Cherry & Edward Imwinkelried, *A Cautionary Note About Fingerprint Analysis and Reliance on Digital Technology*, Champion, August 2006, at 27, 28 ("If the police suspect that a criminal might have left a fingerprint impression on a particular surface, such as a glass tabletop, they can use techniques such as the application of special powders to visualize the image. When they find an image, they photograph it for comparison with the images in the library of fingerprint cards. . . . The law enforcement community is making extensive use of digitized technology in its fingerprint systems. In many cases, if the police succeed in visualizing a latent print at the crime scene, they use a digital camera to preserve the image.").

Voiceprints are not visual, but prove the point just the same. The first step in voiceprint analysis is obtaining a recording of the subject's voice. *See* Paul F. Rothstein, *Federal Rules of Evidence*, Rule 702, Practice Comment (I)(F) (3d ed., Dec. 2014) ("Voiceprint evidence attempts to identify a voice connected with a crime, by a process of reducing a recording of it to an electronically produced pictorial display and comparing it with a similar pictorial display of a known voice or series of voices.").

Google's interpretation of BIPA as inapplicable to face scans collected from photographs is contrary to the very nature of biometric technology and thus would undermine the statute's core purpose. Even in "in-person" collection, photographs of a face are the exact materials used to map out the unique geometric patterns that establish an individual's identity. Taken to its logical conclusion, Google's argument would exclude all the biometric identifiers from the definition of biometric identifiers, because they are all based on the initial capture of a photograph or recording. The legislature could not possibly have intended to expressly enumerate a series of "biometric identifiers," only to effectively exclude them in the following sentence because they are each

derived from a photograph or recording. *See Jordan*, 2015 WL 4498909, at *2 ("[T]he interpretation of a statute must be grounded on the nature and object of the statute, as well as the consequences which would result from construing it one way or another. Legislative intent may be ascertained from the reason and necessity for the act, the evils sought to be remedied, and the objects and purposes sought to be obtained.") (citation omitted).

The "evil[] sought to be remedied" by BIPA, *Jordan*, 2015 WL 4498909, at *2, is private industry's presumptuous arrogation of the right to apply hi-tech tools of measurement and analysis to create identifiers of private individuals without authorization. That is exactly what happened to Plaintiffs Rivera and Weiss, and it makes no difference that their pictures were obtained second-hand from a third party who took or uploaded the image on which Google based its illegal face scan. Indeed, Google's interpretation would deny BIPA's promise of privacy precisely where it is needed most. The statute prohibits gathering biometric identifiers without consent. 740 Ill. Comp. Stat. 14/15(b). If an individual subjected himself or herself to an in-person photography session with Google, which is in the business of biometric identification through face-matching, it might be hard to deny that the individual had given consent, written or otherwise. The greatest evil occurs when privacy-invading operators like Google obtain an individual's picture and create a biometric identifier without his or her consent, as happened here. By Google's logic, nothing would stop it from amassing a tremendous, Orwellian electronic database of face scans with no permission whatsoever so long as the database was derived from photographs. And indeed, that appears to be exactly what it is doing. The Illinois legislature has it right. The practice is offensive to reasonable

expectations of privacy.[4] The statute should not be held inapplicable to the most compelling case for its application.

The Complaints state a claim, and the Motion to Dismiss should be denied.

b. The Legislative History

Google contends that Plaintiffs' claims are inconsistent with the legislative history of BIPA. The argument is completely without merit. The legislative history further confirms that BIPA prohibits Google's unauthorized activities.

The statute itself explains that regulation of biometrics is necessary because they embody an individual's immutable biological characteristics, and thus, unlike other identifiers such as social security numbers, cannot be changed in the event of a security breach:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 Ill. Comp. Stat. 14/5(c). The statute notes that "[t]he full ramifications of biometric technology are not fully known," *id.* 14/5(f), and concludes that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information," *id.* 14/5(g). On its face, the statute expresses a general intent to regulate and protect biometrics, for the purpose of preventing an irreversible security breach that would permanently expose an individual to identity theft and other evils.

---

[4] Google's biometrics database could ultimately be hacked or otherwise wind up in the hands of a nefarious actor who uses the data in a way that it was not intended. Google, unfortunately, cannot guarantee the security of that data any more than Target, Sony, or the Office of Personnel Management were able to ensure the security of their electronically-stored data. BIPA was intended to prevent this risk of harm to innocent individuals by prohibiting companies from collecting and storing biometric data without consent. This is a laudable and legitimate legislative objective.

Google argues that the statute was enacted only to address the "growing" use of "in-person scans" (Mot. at 10 (quoting 740 Ill. Comp. Stat. 14/5(b)), to "access finances or other sensitive information." (*id.* (quoting 740 Ill. Comp. Stat. 14/5(a), (c)). This is a remarkably sloppy misreading of the statute. Financial transactions are merely settings in which compromised biometrics might be misused. It would make no sense to safeguard biometrics only in those settings. Stolen identification – whether a social security number or a scan of face geometry – is a security threat no matter how, when, or where it was stolen. Google might as well argue that the theft of a wallet matters only if it occurs at a cash register, or that the theft of social security numbers matters only if it occurs in the context of a banking transaction. The argument is nonsense. The statute evinces no such crippling restriction on the regulatory scheme. Rather, the statute sensibly expresses a general, unrestricted intent to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information," *id.* 14/5(g), to prevent all of the evils that may result from a breach of personal-identification security.

Google's attempt to emasculate the regulatory scheme is so illogical that it suggests the company simply has contempt for any law that interferes with the company's insatiable appetite for acquiring and exploiting personal information – the crux of the company's business model.[5] *See*

---

[5] Google's contempt for such laws is further demonstrated by the events leading up to the proposed amendment to BIPA that was introduced on May 26, 2016. *See generally* Conor Dougherty, *Tech Companies Take Their Legislative Concerns to the States*, The New York Times (May 27, 2016) (available at http://www.nytimes.com/2016/05/28/technology/tech-companies-take-their-legislative-concerns-to-the-states.html?_r=0) (discussing proposed amendment, and noting that it is "no longer being considered" after various groups "condemn[ed] the proposal"). Google proudly attaches the proposed May 26, 2016 amendment to its Motion to Dismiss, and says that the proposed amendment was motivated by an "inten[tion] merely to clarify the language of BIPA." (Mot. at 3 n.3 (quoting Ex. A to Mot.).) That is simply not true given what we now know.

Immediately after news of the amendment broke, many "suspect[ed] Google or Facebook to be behind the last-minute proposal to change the law." Russell Brandom, *Someone's Trying to Gut America's Strongest Biometric Privacy Law*, The Verge (May 27, 2016) (available at http://www.theverge.com/2016/5/27/11794512/facial-recognition-law-illinois-facebook-google-snapchat). And it appears they were right. Documents filed with the Illinois Secretary of State (Lobbying Index

Randy Stross, *Planet Google: One Company's Audacious Plan to Organize Everything We Know*, at p. 10 (Sept. 18, 2008) (recounting Google's 2006 statement that "[w]e plan to . . . get all of the world's information, not just some."). Here, Plaintiff Rivera is not even among those who have given Google personal information; Plaintiff Rivera has chosen not to submit personal information, yet Google has taken it anyway, in plain violation of BIPA.

Google additionally claims that amendments to the bill that became BIPA indicate the legislature "did not intend the statute to cover facial recognition technology broadly – only the specific, in-person scans that had prompted it to legislate in the first place." (Mot. at 11.) The successive iterations of the bill, however, merely streamlined the eventual statutory language and did not alter its applicability to the scans of face geometry at issue in this case. Google cites the Senate bill's definition of biometric identifiers as progressing from (1) "'any indelible personal physical characteristics'" including but not limited to, *inter alia*, "'records of hand or facial geometry'" (Mot. at 10 (quoting Senate Bill 2400, § 10 (Feb. 14, 2008) (emphasis omitted))), to (2) "'any indelible personal physical characteristics'" including but not limited to, *inter alia*, "'records or scans of hand geometry, facial geometry, or facial recognition'" (*id.* at 11 (quoting Senate

---

Department) reveal that Google, shortly after rolling out its new Google Photos service that is the subject of this lawsuit in mid-2015, began aggressively lobbying the Illinois legislature on "matters affecting Internet related products and services." (*See* Composite Exhibit "A" hereto, at 5.) On August 21, 2015, for example, Google spent $5,000.00 on a "reception for members of the Illinois General Assembly." (*Id.* at 7.) And on October 13, 2015, Google handed out all-expense paid trips to its Mountain View, California headquarters to five Illinois state senators and state representatives, including Elaine Nekritz, State Representative (Chair of the Judiciary-Civil Committee, and Chief Co-Sponsor of SB2400, the bill that became BIPA) and Michael E. Hastings, State Senator (Vice-Chair of the Senate Judiciary Committee, and Chair of the Judiciary Subcommittee on Special Issues). (*See id.* at 13-46.) After these state senators and representatives met and dined with Google for two days, to the tune of $1,679.93 each (*see id., e.g.,* at 57) -- for Google's stated purpose of building "goodwill" (*e.g., id.* at 6) in "matters affecting Internet related products and services" (*id.* at 5) -- all five were shuttled fifteen minutes across town to Facebook's Menlo Park, California headquarters, to attend additional meetings with Facebook that were likewise intended to build "goodwill" (*e.g., id.* at 52) in the area of "[d]evelopments relating to internet regulation and social media," (*id.* at 50).

Against this backdrop, it appears that the proposed May 26, 2016 amendment to BIPA was far less about "clarify[ing] the language of BIPA" (Mot. at 3 n.3) than it was about Google and Facebook trying to achieve extrajudicially what they knew they could not achieve through legitimate advocacy in the courts.

Amendment to Senate Bill 2400, § 10 (Apr. 11, 2008) (emphasis omitted))). The Illinois House of Representatives then replaced the Senate definition with a more concise definition stating that "biometric identifier" means, *inter alia*, "scan of hand or face geometry."

According to Google, by replacing "records" with "scan," and by not adding "facial recognition" alongside "face geometry," the legislature "cared about how the content was obtained" and "only intended the statute to cover . . . in-person scans." (Mot. at 11 (emphasis omitted).) This argument fails for several reasons. First, Google fails to establish that the amendments materially changed the scope of the statute, as opposed to merely refining and streamlining the statutory text. The term "records" was simply unnecessary in view of the statute's clear applicability to "possession," 740 Ill. Comp. Stat. 14/15(a), and to any effort to "collect capture, purchase, receive through trade, or otherwise obtain" biometric identifiers or biometric information, *id.* 14(15(b) – activities that would all necessarily either generate or pertain to some sort of record. Similarly, the term "facial recognition" was unnecessary because a scan of face geometry is a form of "facial recognition" technology; indeed, facial recognition is the entire purpose of a scan of face geometry. The most sensible interpretation of the amendments is mere editorial revision for the sake of clarity and concision. *See, e.g., United States v. Sepulveda*, 115 F.3d 882, 885, n.5 (11th Cir. 1997) (interpreting statute based on plain language, and finding amendments inconclusive, because amendments may be made "'to clarify existing law, to correct a misinterpretation, or to overrule wrongly decided cases,'" such that "'an amendment to a statute does not necessarily indicate that the unamended statute meant the opposite'" (quoting *Hawkins v. United States*, 30 F.3d 1077, 1082 (9th Cir. 1994))).

Second, the Complaints allege specific unauthorized acts and omissions involving scans of face geometry. Those allegations must be accepted as true for purposes of the present Motion to

Dismiss. Google cannot recast the Complaints as reciting activities involving an ill-defined class of unregulated material that Google has concocted for litigation purposes, when the Complaints specifically allege acts and omissions pertaining to scans of face geometry. Even if anything had been left behind in the legislative process (which is not so), scans of face geometry were not, and any effort by Google to disprove the Complaints' allegations raises a question of fact that cannot be resolved on a motion to dismiss.

The Complaints state a claim, and the Motion to Dismiss should be denied.

II. Google Violated BIPA in Illinois Because the Circumstances Relating to Google's Unauthorized Collection of Plaintiffs' Scans of Face Geometry Occurred Primarily and Substantially Within Illinois.

Google's alternative argument for dismissal – that the Complaints "fail[] to allege a violation of BIPA in Illinois" and thus improperly exceed the geographical scope of the statute (Mot. at 13) – is likewise without merit. Google conveniently ignores the overwhelming majority of circumstances relating to Plaintiffs' claims that occurred in Illinois.

In Illinois, "a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E. 2d 801, 853 (2005) (citing, *inter alia*, *Dur–Ite Co. v. Industrial Comm'n,* 394 Ill. 338, 350 (1946)). Because the express provisions of BIPA evince no such intent, only violations of BIPA that "take place" inside Illinois are actionable. *See id.*

The Illinois Supreme Court's decision in *Avery* conclusively demonstrates that the claims alleged in the Complaints took place in Illinois. In *Avery,* the Illinois Supreme Court addressed whether a class of insureds, who were challenging the defendant's practice of using non-OEM crash parts to repair policyholders' cars, could sue under the Illinois Consumer Fraud Act ("ICFA"). The court held that "a plaintiff may pursue a private cause of action under the [ICFA] if

the circumstances that relate to the disputed transaction occur primarily and substantially in Illinois." *Avery*, 835 N.E. 2d at 854 (emphasis added). "[T]here is no single formula or bright-line test for determining whether a transaction occurs within this state." *Id.* "Each case must be decided on its own facts." *Id.* In determining whether a transaction occurred primarily and substantially in Illinois, courts consider such factors as "the place of injury or deception, the location of the parties, the location where the relevant activities occurred, and the parties' contacts with Illinois." *Valley Air Serv. v. Southaire, Inc.,* No. 06 C 782, 2009 WL 1033556, at *12 (N.D. Ill. Apr. 16, 2009) (citing *Avery,* 296 Ill. Dec. 448, 835 N.E.2d at 853–55); *see also, e.g., The Clearing Corp. v. Fin. and Energy Exchange Ltd.,* No. 09 C 5383, 2010 WL 2836717, at *6 (N.D. Ill. July 16, 2010).

In this case, the circumstances that relate "to the disputed transaction" – i.e., to Google's failure to obtain informed written consent from Plaintiffs prior to collecting their scans of face geometry[6] -- "occur[ed] primarily and substantially in Illinois." *Id.* at 854. Plaintiffs are both Illinois residents. (*Rivera* Compl. ¶ 7; *Weiss* Compl. ¶ 7.) Google markets and sells its Droid devices to consumers in Illinois. (*Rivera* Compl. ¶ 27; *Weiss* Compl. ¶ 27.) Plaintiffs' photos were taken in Illinois with Droid devices purchased in Illinois. (*Rivera* Compl. ¶ 27; *Weiss* Compl. ¶ 28.) Immediately after Plaintiffs' photos were taken in Illinois, Plaintiffs' photos were automatically uploaded in Illinois to the cloud-based Google Photos service, from an Illinois-based Internet Protocol ("IP") address. (*Id.*) Immediately upon the upload of Plaintiffs' photos, Google collected Plaintiffs' scans of face geometry. (*Rivera* Compl. ¶¶ 28, 34; *Weiss* Compl. ¶¶ 29, 35.) Google failed to provide Plaintiffs with written disclosures in Illinois and failed to obtain Plaintiffs' written

[6] Post-*Avery* decisions of the Illinois Supreme Court confirm that Google's failure to make the required disclosures and obtain written consent prior to collecting Plaintiffs' scans of face geometry is the conduct analogous to the "disputed transaction" at issue in *Avery*. *See, e.g., Gridley v. State Farm Mut. Auto. Ins. Co.*, 840 N.E. 2d 269, 274-75 (2005) (citing *Avery*, 835 N.E. 2d at 801) (explaining that "Avery's estimate for repairs to his car was written in Louisiana and the alleged deception—the failure to disclose the inferiority of non-original-equipment-manufacturer parts—occurred in Louisiana.").

consent in Illinois prior to collecting their scans of face geometry (*Rivera* Compl. ¶¶ 31-33; *Weiss* Compl. ¶¶ 32-34); indeed, both of these statutory prerequisites to the collection process should have occurred in Illinois because Plaintiffs were present in Illinois when the photos were uploaded and their scans of face geometry were collected. Because the overwhelming majority of circumstances relating to Google's unauthorized collection of Plaintiffs' biometrics occurred in Illinois, the Complaints clearly allege BIPA claims that took place in Illinois. *See, e.g., Jamison v. Summer Infant (USA), Inc.*, 778 F. Supp. 2d 900, 910 (N.D. Ill. 2011) (pursuant to *Avery*, plaintiff "clearly ha[d] standing" to sue under ICFA because plaintiff was resident of Illinois, purchased underlying product at a store in Illinois and used the products in Illinois, and because defendants "marketed and sold" the products in Illinois, notwithstanding fact that defendants' "principal place of business [was] outside of Illinois"); *cf., e.g., Avery*, 835 N.E. 2d at 854 (concluding that because the "overwhelming majority of circumstances relating to the disputed transactions in this case—State Farm's claims practices—occurred outside of Illinois for the out-of-state plaintiffs[,]" plaintiffs "have no cognizable cause of action under the Consumer Fraud Act."); *Int'l Profit Associates, Inc. v. Linus Alarm Corp.*, 971 N.E. 2d 1183, 1194 (2012) (IFCA claim did not occur in Illinois because "the claimant's residence is in Florida, the location of the deception was in Florida, the damages sought in the counterclaim occurred in Florida, and almost all of the communication related to the fraud claims occurred in Florida.").

Google pins its entire extraterritoriality argument on the Complaints' failure to allege that Google actually extracts scans of face geometry from photographs in Illinois. But the physical location of Google's illegal face scan extraction apparatus is merely one factor among many under the *Avery* analysis, and is by no means dispositive. *See Gross v. Midland Credit Mgmt.*, 525 F. Supp. 2d 1019, 1024 (N.D. Ill. 2007) (explaining that, under *Avery*, "it is … incorrect to focus on only one

aspect of the disputed transaction"); *see also, e.g., Jamison*, 778 F. Supp. 2d at 910 (circumstances relating to claim primarily and substantially occurred in Illinois, even though defendant's "principal place of business [was] outside of Illinois"); *cf., e.g., Avery*, 835 N.E. 2d at 854 (circumstances relating to claim did not primarily and substantially occur in Illinois, even though defendant was located in Illinois).

In *Gross*, for example, the defendant argued that the disputed transaction took place outside of Illinois because the defendant was located in Arizona and the transaction was negotiated between defendant's representatives in California and Arizona. In rejecting the defendant's argument, the district court explained:

> *Avery* instructs courts to consider the totality of the circumstances in determining whether the disputed transaction occurred 'primarily and substantially' in Illinois. *Id.* at 854. It is therefore incorrect to focus on only one aspect of the disputed transaction. Ford Credit's argument discounts the importance of such factors as Gros' residence, the location of the alleged harm, the site of Gros' dealings with Ford Credit, the Illinois court case, and the site of Gros' communications with MCM – all of which are 'circumstances relating to [the] disputed transaction.' *Id.* Furthermore, because Niepage's affidavit goes beyond the scope of Gros' Amended Complaint, the court will not consider this evidence in addressing Ford Credit's Motion to Dismiss. *See Loeb Indus., Inc. v. Sumitomo Corp.,* 306 F.3d 469, 479 (7th Cir.2002). At this point in the proceedings, based on the allegations in Gros' Amended Complaint, the court declines to find that the circumstances surrounding Gros' claim occurred primarily and substantially outside of Illinois.

Id. at 1024-25. Likewise in this case, the location of the apparatus used to extract Plaintiffs' scans of face geometry is just one aspect of Google's illegal biometrics collection operation. Google ignores Plaintiffs' residence, the location of the marketing and sale of the Droid devices at issue, the location of Plaintiffs' interactions with Google (i.e., where Plaintiffs were located at the time their photographs were taken and uploaded), the location corresponding to the IP addresses from which Plaintiffs' photographs were uploaded, and the location of the alleged harm (i.e., where Google

failed to obtained informed written consent prior to extracting and collecting Plaintiffs' scans of face geometry) – all of which are "circumstances relating to the disputed transaction" that occurred in Illinois.

Google contends that the proposed class definitions call for an extraterritorial application of the statute. (Mot. 13-14.) However, the Motion to Dismiss is limited to challenging the legal sufficiency of the claims alleged by Plaintiffs Rivera and Weiss individually. The proposed class definitions are just that – proposals – and are subject to change prior to class certification. *See Robidoux v. Celani,* 987 F.2d 931, 937 (2d Cir. 1993) (holding that "a court is not bound by the class definition proposed in the complaint"). Accordingly, any objection Google has to the class definitions must be raised in opposition to Plaintiffs' motions for class certification, not at the pleadings stage. *See Lucas v. Ferrara Candy Co.*, No. 13 C 1525, 2014 WL 3611130, at *8 (N.D. Ill. July 22, 2014) (explaining that objections to class definitions should be "raised through opposition to a plaintiff's motion to certify a class rather than in a motion to dismiss"); *Howard v. Renal Life Link, Inc.*, No. 10 C 3225, 2010 WL 4483323, at *2 (N.D. Ill. Nov. 1, 2010) (explaining that motion to dismiss is not the proper venue for objecting to class definition, and collecting cases); *see also, e.g., Oxman v. WLS–TV*, 595 F. Supp. 557, 561–62 (N.D. Ill. 1984) (motion to dismiss was premature because issues would be better raised in motion opposing class certification).

Even if the Court considers the propriety of the proposed class definitions at this stage of the proceedings, the geographical scope of the proposed class claims is consistent with that of Plaintiffs' individual claims (which allege violations of BIPA in Illinois, as discussed above). The Complaints allege that Google Droid devices automatically and immediately upload photos after they are taken, and that Google automatically and immediately thereafter collects scans of face geometry from those photos. (*Rivera* Compl. ¶¶ 21-22, 27-28, 34; *Weiss* Compl. ¶¶ 21-22, 28-29,

35.) It necessarily follows, then, (1) that the individuals appearing in photos uploaded in Illinois from Droid devices were present in Illinois at the time the photos were taken; (2) that Google collected scans of face geometry from those individuals while they were present in Illinois; and (3) that Google could have provided written disclosures to those individuals in Illinois and obtained written consent from those individuals in Illinois, but failed to do so. Accordingly, even under the current proposed class definitions, the circumstances relating to the claims of the putative class members occurred "primarily and substantially" in Illinois. *See Avery*, 835 N.E. 2d at 854.

The Complaints state a claim, and the Motion to Dismiss should be denied.

III. BIPA Does Not Violate the Dormant Commerce Clause Because the Statute Does Not Impact Commerce Outside Illinois.

Finally, Google argues that "if the presumption against extraterritoriality does not clearly exclude Google Photos from BIPA's reach, then BIPA would violate the dormant commerce clause." (Mot. At 15.) This argument is without merit because, as the Complaints demonstrate, Google's compliance with BIPA poses no risk of burdening interstate commerce whatsoever.

The commerce clause both affirmatively grants power to Congress to regulate interstate commerce but also implies a negative converse – "a substantive 'restriction on permissible state regulation' of interstate commerce." *Dennis v. Higgins*, 498 U.S. 439, 447 (1991) (quoting *Hughes v. Oklahoma,* 441 U.S. 322, 326 (1979)); *see also S.-Cent. Timber Dev., Inc. v. Wunnicke*, 467 U.S. 82, 87 (1984) ("[T]he Clause has long been recognized as a self-executing limitation on the power of the States to enact laws imposing substantial burdens on such commerce."). This negative implication – that states may not take actions that unduly interfere with the affirmative power of the federal government to regulate interstate commerce – is generally known as the "dormant commerce clause." *See CTS Corp. v. Dynamics Corp. of America*, 481 U.S. 69, 87 (1987).

"In considering whether a state regulation violates the commerce clause, a court first

determines if the regulation directly discriminates against interstate commerce or has the effect of favoring in-state economic interests; if so, the state regulation is generally struck down." *Hirst v. Skywest, Inc.*, No. 15 C 02036, 2016 WL 2986978, at *10 (N.D. Ill. May 24, 2016) (citing *Brown-Forman Distillers Corp. v. New York State Liquor Auth.*, 476 U.S. 573, 578-79 (1986); *Nat'l Solid Wastes Mgmt. Ass'n v. Meyer*, 63 F.3d 652, 657 (7th Cir. 1995)). If the state regulation is neutral on its face or only has indirect effects on interstate commerce, the regulation "will be upheld 'unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.'" *Nat'l Solid Wastes*, 63 F.3d at 657 (quoting *Pike v. Bruce Church, Inc.,* 397 U.S. 137, 142 (1970)).

Because BIPA does not "directly discriminate[] against interstate commerce or ha[ve] the effect of favoring in-state economic interests," *Hirst*, 2016 WL 2986978, at *10, Google must demonstrate that BIPA imposes a burden on interstate commerce that "is clearly excessive in relation to the putative local benefits," *Nat'l Solid Wastes*, 63 F.3d at 657. Google completely fails this test. Google not only fails to establish any burden that BIPA imposes on interstate commerce, it fails to articulate how any such burden is excessive in relation to BIPA's benefits to Illinois.

Google contends that BIPA violates the dormant commerce clause because the "practical effect" of the statute is "to control conduct beyond the boundaries" of Illinois. (Mot. at 15 (citing *Healy v. Beer Inst., Inc.,* 491 U.S. 324, 335-37 (1989)).) This argument is a straw man that rests entirely on the following inapposite hypothetical:

> Suppose a Google Photos user who lives in Wisconsin takes a photograph of a friend from Iowa and sends it to her friend who lives in Indiana. The Indiana resident receives and uploads the photograph while driving through Illinois, and then Google creates a face template from the photograph on servers in another state. According to Plaintiffs, Illinois can regulate what Google does with the photograph based on an exceedingly tenuous and fortuitous connection—the fact that a user happened to upload it to Google's cloud servers while passing through Illinois. According to Plaintiffs, regardless of the policies of the three other states at issue in this

> scenario, Illinois could project its regulatory power into those other states.

(Mot. at 15.)

Google's hypothetical has no bearing on the factual allegations of the Complaints with respect to the named Plaintiffs. As discussed above, the Google Photos users who took the photographs in this case lived in Illinois. The photographs were taken in Illinois and depicted individuals in Illinois. The photographs were automatically uploaded to Google in Illinois. Google failed to obtain informed written consent from the individuals depicted in the photographs in Illinois. Based on these factual allegations, the "practical effect" of the statute is to control conduct occurring entirely within Illinois. *See Healy,* 491 U.S. at 335. Thus, the scenario that Google has concocted for litigation purposes has no relevance to the claims alleged in the Complaints.

Moreover, the proposed class definitions, which encompass individuals appearing in photographs uploaded in Illinois, are consistent with the claims alleged by Plaintiffs Rivera and Weiss. The Complaints allege that Google Droid devices automatically and immediately upload photos after they are taken, and that Google automatically and immediately thereafter collects scans of face geometry from the individuals depicted in those photos. (*Rivera* Compl. ¶¶ 21-22, 27-28, 34; *Weiss* Compl. ¶¶ 21-22, 28-29, 35.) Therefore, when a photograph is uploaded from a Droid device in Illinois, the individuals depicted are necessarily present in Illinois at the time Google collects its illegal scans of face geometry. Likewise, when a photograph is uploaded from a Droid device in Illinois, Google necessarily fails to provide the requisite disclosures or obtain the requisite written consent in Illinois. Again, the "practical effect" of the statute as applied to the putative class claims is to control conduct occurring entirely within Illinois. *See Healy,* 491 U.S. at 335.[7]

---

[7] To the extent the class definitions encompass Google's hypothetical – i.e., includes individuals appearing in photographs taken in states other than Illinois that are eventually uploaded to Google Photos in

Google contends that it is "impossible for [it] to ascertain *ex ante* whether a particular photograph is subject to the constraints of BIPA." (Mot. at 16.) That is a question of fact. Google's contention is also entirely incorrect. Google can determine whether a particular photograph is subject to the regulations of BIPA – that is, whether a photograph is uploaded from within Illinois – by analyzing whether an Illinois-based IP address is associated with the device uploading the photograph. *See F.T.C. v. Asia Pac. Telecom, Inc.*, 788 F. Supp. 2d 779, 786 (N.D. Ill. 2011) ("IP addresses correspond to the geographic location of an Internet connection[.]"); *United States v. Upshaw*, No. CRIM. 12-299 MJD/LIB, 2013 WL 1104759, at *1 n.6 (D. Minn. Feb. 5, 2013) (an IP address is "unique to a particular computer during an online session" and "identifies the location of the computer with which the address is associated."); *see also, e.g., Pacific Century Int'l, Ltd. v. Does 1-37*, 282 F.R.D. 189, 195–96 (N.D. Ill. 2012) (quashing subpoena to internet service provider seeking identities of IP address users engaged in illegal downloading that were not located specifically in the Northern District of Illinois); *United States v. Dreyer*, 767 F.3d 826, 834 (9th Cir. 2014) (recounting government agent's "standard practice" of using IP addresses to locate and then monitor "all computers in a geographic area, here, *every* computer in the state of Washington").

Google, of course, knows this full well. In response to European Union privacy regulations, Google has already limited its collection of scans of face geometry to photographs uploaded from certain countries (beginning with the United States, with gradual expansion elsewhere), and does so by using IP addresses to determine the geographical locations of incoming photographs. *See* James Vincent, *Facebook's New Photo App Won't Launch In Europe Because of Facial Recognition*, The Verge, http://www.theverge.com/2015/6/19/8811617/facebook-moments-facial-recognition-europe (June 19, 2015) ("Google's recently-launched Google Photos app — which uses

---

Illinois – and to the extent such a situation implicates the dormant commerce clause, then the class definitions can be modified at the appropriate stage of the proceedings.

facial recognition to sort snaps by who's in them — also limits its use of the technology to the US."); *Updates & Announcements for Oct. 28, 2015*, Google Photos, https://plus.google.com/+GooglePhotos/posts/EPjgwrsrRyF ("Rolling out on all platforms, here's what's new: … Face grouping will be available in Latin America, Canada, the Caribbean, Australia, and New Zealand. It will also be available in parts of Asia, the Middle East, and Africa."); Jason Bouwmeester, *HOW TO; Enable the "Group Similar Faces" People Function in Google Photos*, Techaeris, http://techaeris.com/2015/05/31/how-to-enable-the-group-similar-faces-people-function-in-google-photos/ (May 31, 2015) (explaining that Google Photos facial recognition technology is only available on devices that have "a U.S. IP address").[8]

Thus, contrary to the Motion to Dismiss, Google has the ability to comply with BIPA in Illinois in the same way it has complied with European Union privacy regulations overseas – by using IP addresses and other geo-tracking data to limit its biometrics collection practices to photographs uploaded from the 49 states other than Illinois. Google cites no legal authority, nor is there any, demonstrating that such an approach would result in Illinois projecting its regulatory policies into other states in violation of the dormant commerce clause.

CONCLUSION

For the foregoing reasons, the Court should deny the Motion to Dismiss (D.E. 49) in its entirety.

---

[8] Google also tracks the IP addresses of its users in order to deliver personalized content based on location. *See* Alexandra D. Vesalga, *Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data*, 43 Golden Gate U. L. Rev. 459, 465 (2013) ("Google's search engine reads a user's location via his or her IP address to automatically return suggested, locationally relevant search results."); John Schinasi, *Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion*, 52 Colum. J. Transnat'l L. 569, 574 (2014) (discussing Google's "ability to geographically locate a user via signals such as IP location, Wi-Fi networks, or GPS without her consent.").

Dated: July 1, 2016

Respectfully submitted,

/s/ Katrina Carroll

Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
LITE DEPALMA GREENBERG, LLC
211 West Wacker Drive, Suite 500
Chicago, Illinois 60606
Telephone: (312) 750-1265

AHDOOT & WOLFSON, PC
Robert Ahdoot
radhoot@ahdootwolfson.com
Tina Wolfson
twolfson@ahdootwolfson.com
Bradley King
bking@ahdootwolfson.com
1016 Palm Avenue
West Hollywood, California 90069
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

CAREY RODRIGUEZ
MILIAN GONYA, LLP
David P. Milian
dmilian@careyrodriguez.com
Frank S. Hedin
fhedin@careyrodriguez.com
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474
Facsimile: (305) 372-7475

Counsel for Plaintiff and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on July 1, 2016, I electronically filed the foregoing with the Clerk of Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record via transmission of Notices of Electronic Filing generated by CM/ECF.

/s/ Katrina Carroll
Katrina Carroll